CHAPTER 1

INTEGRATING PUBLIC SAFETY NETWORKS TO 5G: APPLICATIONS AND STANDARDS

Abstract

Public Safety Networks (PSNs) and commercial cellular networks evolved in isolation having divergent goals. The primary goal of PSNs was to enable mission-critical voice services among first responders. On the other hand, commercial cellular networks are aimed at providing voice, video, and data services to a broad range of customers. In recent years, the Public Safety (PS) agencies came across many situations when they were unable to share critical information among themselves due to narrowband and incompatible nature of the networks they operate in. For instance, PSN operated by police is incompatible with the one operated by the fire brigade and other similar PS agencies. To overcome this issue, an initiative has been taken to come-up with an interoperable integrated broadband PSN. Indeed, different Standards Developing Organizations (SDOs), including the 3rd Generation Partnership Project (3GPP), are playing their roles for a smooth transition of PSNs to evolved 5G networks. In this chapter, we survey the efforts of those SDOs, highlighting various challenges they are facing.

Please enter `\offprintinfo{(Title, Edition)}{(Author)}` at the beginning of your document.

1.1 Introduction

Reliable and robust communication networks are fundamental for Public Safety (PS) agencies to provide services for Public Protection and Disaster Relief (PPDR). Historically, Public Safety Networks (PSNs) and commercial mobile broadband evolved in isolation, pursuing divergent goals. PSNs transitioned from analog systems of 20^{th} century to today's digital narrowband systems, deployment of which started back in 1990s. Their main focus was *mission-critical* voice services that enable communication between emergency first responders in one-on-one fashion or within a group with the help of deployed infrastructure or even without it. However, their narrowband nature does not permit high data-rate multimedia services such as video that is instrumental for providing effective PPDR services.

Commercial broadband networks evolved in parallel but experienced a spectacular technological revolution mostly driven by high profitability and large market size due to a wider public audience. As a result, techniques for efficient radio resource utilization over a broadband spectrum made them well-suited for high data rate services including voice, video, etc. However, unlike narrowband PS networks, these technologies provide *non-mission-critical* and often only one-to-one communication. The support for group communications remained very basic, meeting far less stringent constraints than those required for traditional PS networks.

A brief history of transition of PSNs from the analog system to future 5G networks is summarized in Table 1.1. To conduct their day-to-day operations, PS agencies combined complementary strengths of mission-critical PS networks and more pervasive commercial cellular networks. But, lack of a single communication system in the field operations led to both operational and technological inefficiencies such as slower response time and sub-optimal spectrum usage. To overcome these limitations, different Standards Developing Organizations (SDOs) have made strides recently in proposing standards to support the convergence of both kinds of networks.The latest major advancement in this area is done by 3GPP through ratification of the 5G.

In foreseeable future, PS agencies are expected to adopt broadband PS networks, while legacy narrowband networks will still coexist for a smoother transition during infrastructural and operational changes. This chapter summarizes standardization efforts made to support an inevitable convergence of PS communication networks across multiple regions. Further, we anticipate that this convergence will not be limited to narrowband and broadband technologies but will also be influenced by recent trends on how people access information today. Over the past few decades, information access methods have extended well beyond basic telephony. An on-going wave of revolution in emerging technologies like massive Internet-of-Things (IoT), crowdsourcing, Online Social Networks (OSNs), Wireless Sensor Networks (WSNs), and many others combined with industry's push towards transition of communication systems to "All IP" based networks will change the landscape of future public safety networks. All these trends are bound to blend into impending narrowband-broadband convergence for PS networks.

TABLE 1.1 A brief history and evolution of public safety networks.

1923	First two-way radio developed
1939	First Walkie-Talkie designed
1941	First two-way radio system by Motorola deployed in Philadelphia, Pennsylvania, USA
1976	First group communications in PSN
1988	Initiative to migrate analog PSNs to digital PSNs
1989	First digital PSN APCO Project 25, came into existence in USA
1995	TETRA came into existence in Europe
2005	DMR standardized by ETSI
2013	FirstNet LTE deployment started
2015	Support ProSe services and group communications for public safety applications in 3GPP release 12
2016	Support for mission critical push to talk for public safety applications in 3GPP release 13
2017	Support for multimedia broadcast supplement for public warning system in 3GPP release 14.

We envision that future PS networks will be an inclusive system that will glue different broadband and narrowband technologies along with other emerging technologies mentioned above. In this grand scheme, technology will enable the general public to get more involved in delivering their collective responsibility towards PS. Moreover, this chapter highlights different challenges to achieve this vision with some future directions.

The rest of the chapter is organized as follows: In Section 1.2, we discuss possible public safety scenarios in future 5G networks. Section 1.3 describes the standardization process of integrating legacy PSNs to commercial cellular networks. In Section 1.4, we present potential challenges and enabling technologies for this integration. Finally, Section 1.5 concludes this chapter.

1.2 Public Safety Scenarios

The 3rd Generation Partnership Project (3GPP) presents different use cases and scenarios for public safety applications, mainly based on the coverage area of cellular networks. These scenarios are presented to support National Security and Public Safety (NSPS) services using Device to Device (D2D) communications in next-generation cellular networks Usman, Gebremariam, Granelli & Kliazovich (2015), Usman, Gebremariam, Raza & Granelli (2015). These scenarios can be categorized into three distinct types, which are elaborated in Figure 1.1.

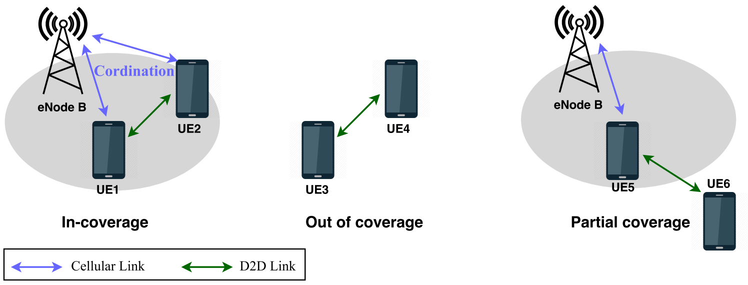

Figure 1.1: Supported scenarios for ProSe.

1.2.1 In-coverage Scenario

In this scenario, all User Equipments (UEs) could lie in the coverage area of the cellular network. The network operator is fully responsible to control all functionalities of D2D communications, such as device discovery, device configuration, identity authentication, resource allocation, connection establishment and termination, access control, and security management. In this scenario, the D2D links are established in the same licensed spectrum on which UEs are connected to the Base Station (BS). In other words, UE-to-UE communications and UE-to-BS communications share the same licensed spectrum.

1.2.2 Out-of-coverage Scenario

In this scenario, all UEs are located outside the coverage area of the cellular network. The devices can establish D2D links without any assistance from the infrastructure. This use-case is the practical application of the disaster scenarios, where the cellular infrastructure is completely or partially damaged and a part of the network is offline. For example, in Figure 1.1, UE3 and UE4 can establish D2D links and start their communication without any support from the infrastructure. In this scenario, the UEs are responsible to control most of the functionalities of D2D communications, such as device discovery, device configuration, identity authentication, connection establishment and termination, access control, and security management. In 3GPP standardization procedures, communication in the out-of-coverage scenario is available for PS UEs only, while commercial UEs cannot avail this service.

1.2.3 Partial-coverage Scenario

In this scenario, some UEs are located outside the coverage area of the cellular network. The UEs at the edge of the coverage area relay the information of out-of-coverage UEs to the base station or core network. This helps to extend the coverage area of the network at the edge. For example, in Figure 1.1, UE5 acts as a relay node to extend the coverage of the cellular network to UE6. In this scenario, the network operator is fully responsible to control all functions of D2D communications, such as device discovery, device configuration, identity authentication, resource allocation, connection establishment and termination, access control, and security management, for both UE-to-UE and UE-to-BS communications.

1.3 Standardization Efforts

This section highlights the efforts to standardize the inter-operable broadband technology for PSNs. It is important to note that 3GPP is the main contributor to the standardization process of broadband PSNs. However, 3GPP is not the only contributor. In fact, some other SDOs are also playing an important role to make a smooth transition from narrowband to inter-operable broadband PSNs.

In 2012, the First Responder Network Authority (FirstNet) Farrill (2012) was created in the United States (US) to build, operate, and maintain the first nationwide inter-operable broadband wireless network for PS. The FirstNet, in support with Public Safety Communication Research (PSCR), is coordinating with SDOs for setting standards to advance PS communications and interoperability as shown in Figure 1.2. These SDOs are working towards different aspects of broadband PSNs.

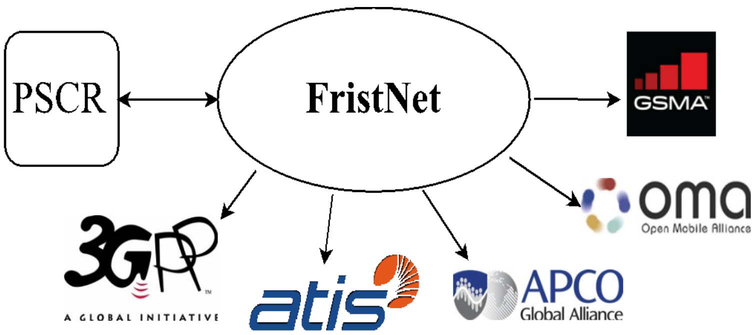

Figure 1.2: FirstNet PS standardization process.

3GPP is mainly responsible for standardizing the broadband supplement of all features that we have in narrowband technology (both for voice and video), e.g., Mission Critical Push-To-Talk (MCPTT), group communications, and Public Warning System (PWS). Similarly, Alliance for Telecommunication Industry Solution (ATIS) is mainly responsible for next-generation E911 and all-IP based solutions for interoperability. On the other hand, Groupe Speciale Mobile Association (GSMA) is providing support for their Voice over LTE (VoLTE) initiative. Moreover, Open Mobile Alliance (OMA) is working on the standardization of Push to Communicate for Public Safety (PCPS). Lastly, The Association of Public-Safety Communications Officials - International, Inc. (APCO International) is committed to make best use of emerging technologies for narrowband Land Mobile Radio (LMR) equipment and systems.

In what follows, we will briefly discuss the role of each SDO towards standardization of broadband PSN.

1.3.1 3rd Generation Partnership Project

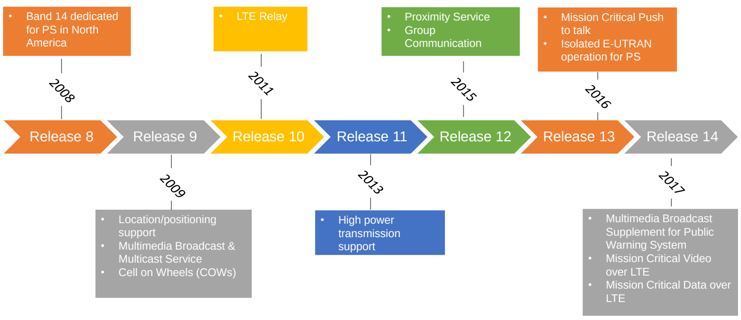

Figure 1.3: Evolution of PS features in 3GPP.

Since the interest of PS community in broadband PSN, 3GPP has been actively participating to ensure a smooth transition of narrowband PSNs to broadband networks (such as 5G). In particular, 3GPP takes the requirements and technical inputs from the standards committees of the narrowband PSN (such as Terrestrial Trunked Radio (TETRA) and Project 25 (P25)) to enhance the LTE technology to support the required features Ferrus & Sallent (2014). Technically, the Technical Specification Groups (TSGs) working on Radio Access Network (RAN) are responsible to enhance the basic functionalities of the access network to support direct D2D communications. However, for the overall applications on top, i.e., voice communications (known as push-to-talk) and group communications, a separate standardization group has been created. This group is called “Service and System Aspects Working Group 6 (SA WG6)”, shortly SA6.

Since LTE is a cellular technology and most of its specifications were completed in 3GPP release 8, so we start from release 8 highlighting PS features.

—-

1.3.1.1 Release 8: 3GPP release 8, completed in December 2008, provided support for LTE band 14, a 20MHz spectrum in 700MHz band, dedicated to PS both in the US and Canada. In addition, the release 8 provided an ability to set up mobile data connection from a device to packet network Parkvall et al. (2011). These are the very basic features of broadband PSNs.

1.3.1.2 Release 9: 3GPP release 9, completed in December 2009, included several enhancements related to PS Parkvall et al. (2011). It provided a support for location-based services and positioning that is critical for first responders to track each other during a mission. The most important PS feature in release 9 was the support of Multimedia Broadcast and Multicast Service (MBMS). It is an enabling technology for group communications and video broadcasting in PSNs. More importantly, Release 9 also provided an emergency calling support, for instance E911, which is critical to ensure public safety. In addition, for PS scenarios, release 9 provided a support for mobile base station, *a.k.a.* Cell on Wheels (COW) in the PS community.

1.3.1.3 Release 10: 3GPP release 10 (LTE-Advanced), completed in March 2011, provided relay support for LTE. This allows a base station, for example, mounted on a fire vehicle to relay information from firefighter in a basement back to the network Buis (2012).

1.3.1.4 Release 11: 3GPP release 11, completed in March 2013, included the support for high power devices in band 14. Generally, the power for normal cellular devices is limited to 200mW, while in this release the power for PS devices was increased to 1.25 Watts. This significantly reduced the network deployment cost, improving coverage area of LTE network for PS scenarios Ahmadi (2013).

1.3.1.5 Release 12: 3GPP release 12 was one of most important the releases that incorporated two very important features of PS communications, *i.e.,* Proximity Services (ProSe) and Group Communications. ProSe, *a.k.a.* D2D communications, is an enabler of direct communication between PS devices, while group communication allows PS users to operate in group, especially when they are on mission Sauter (2017). This release was completed in March 2015.

In what follows, we will briefly describe the main features of ProSe and group communications in LTE release 12.

Proximity Services (ProSe): The proximity services in LTE are about discovering mobile devices in the close physical proximity and enabling communication among them with or without supervision from the LTE network. These services are very critical for PS officials and first responders. In release 12, these services are sometimes described as either “Direct Mode” or “off-network communication”. The system enablers for ProSe services include direct discovery and direct communication, Evolved Packet Core (EPC)-level ProSe discovery, and EPC support for WLAN-based direct discovery and communications.

The scenarios that are supported by direct discovery and direct communications are listed in Table 1.2 and shown in Figure 1.1. Particularly, new network elements

Table 1.2: Supported ProSe functions in 3GPP release 12 to enable D2D communications in public safety and non-public safety applications.

Scenarios	**Within Network Coverage**	**Outside Network Coverage**	**Partial Network Coverage**
Supported Applications	*Supported ProSe Functions*		
Non-Public Safety	Discovery	-	-
Public Safety	Discovery, Communication	Communication	Communication

are added and new interfaces are defined to support ProSe in LTE. A simplified block diagram of overall network architecture, including ProSe functionalities, is shown in Figure 1.4 Roessler (2015). From a direct communication point of view, the most important interface is PC5 interface between two UEs and PC3 interface between the UE and new network node, ProSe function. The information exchange through PC3 interface is mainly based on HTTP that is used as a transport protocol. The ProSe messages are embedded in the body of HTTP Request and Response messages.

For out of coverage scenarios, the most relevant parameters related to PS can be stored in the UE itself, either hardcoded into the UE or in the Universal Integrated Circuit Card (UICC) or Subscriber Identity Module (SIM card). The ProSe function is responsible for the authorization and provision of radio and security parameters for direct communication.

Group Communication: This is one of the most important and frequently used features of PSNs when communicating with multiple users. The group communication is dependent on MBMS services introduced in LTE release 9. In release 9, there was no mechanism to measure the signal quality at the UE needed for providing better tools to monitor and adjust the MBMS operational parameters. This is included in release 12 by adding new measurements (e.g., signal strength, signal-to-noise ratio, and error rate) in radio layer Multicast Broadcast Single Frequency Networks (MBSFN) metric. The MBMS access is made available by the creation of MB2 interface between Group Communication Service Application Server (GCS-AS) and Broadcast Multicast Service Center (BMSC). The MBMS radio resources in a cell are semi-statically allocated according to low activity period in order to not overprovision them uselessly. But, in case of an incident, several PS groups in that cell need to suddenly communicate over those MBMS resources, resulting in a severe overload of these resources. The group communication work item in release 12 provides mechanisms to cope with this overload situation.

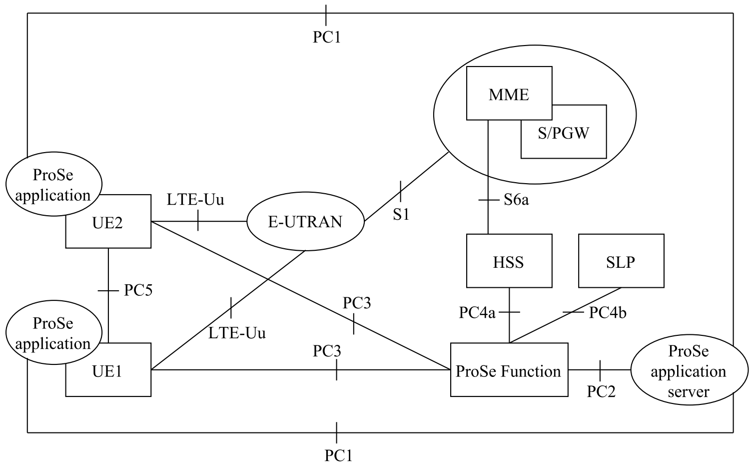

Figure 1.4: D2D ProSe network architecture. Roessler (2015)

1.3.1.6 Release 13: 3GPP release 13 was completed in March 2016. In release 13, several PS features initiated in release 12 were continued for further enhancements Kaleem et al. (2018). For instance, LTE D2D communications and discovery was further enhanced to meet the PS requirements for in-network coverage (inter- and intra-cell), partial network coverage, and outside network coverage scenarios. The non-PS discovery is still limited to in-network coverage only. There are further enhancements to D2D communications to enable the extension of the network coverage using Layer 3 based UE-to-Network relay for partial and outside network coverage scenarios, considering applicability to voice and video. The most important PS features in release 13 are summarized here.

Mission critical push-to-talk over LTE (MCPTT): MCPTT is the key enabler for many PS features, such as person-to-person calls, group calls, group management, user management, security, operation in off-network mode, operation in relay-to-network mode, and many other related features. MCPTT uses ProSe services to enable direct communication between devices, both in and out of LTE network coverage. Current standardization efforts include the development of application layer architecture for MCPTT, defining basic architecture functionalities across applications, and identifying reusable components in existing TETRA, Critical Communications Evolution (TCCE), and OMA PCPS specifications. A PTT application server is proposed as a part of GCS-AS, where GCS is a generic function for voice and data.

Related to MBMS, two areas are specifically enhanced in release 13. One is service continuity and the second is the independence of application from knowing the service areas defined in the network.

Isolated E-UTRAN Operation for PS: To provide voice, video, and data services to PS officials working in an area where backhaul connection is cut-off during mission-critical operation, the isolated E-UTRAN operation for PS is proposed in release 13.

The PS officials may deploy dedicated eNodeB(s) for nearby PS UEs beyond what is provided by UE-to-UE direct communication mode. This requires enabling separate and autonomous security mechanisms for isolated E-UTRANs. In release 13, the isolated E-UTRAN operation for PS comprises of following features: operation with no or limited connection to EPC, multiple isolated eNodeBs with interconnection between them, and the support of local operations like group communication.

1.3.1.7 Release 14: 3GPP release 14 improves the following features of PS communications Hoymann et al. (2016), Kaleem et al. (2018).

Multimedia Broadcast Supplement for Public Warning System (PWS): The purpose of this feature is to enable effective delivery (and broadcasting) of extensive multimedia public warning contents in PWS and investigating mechanisms to enable users to receive and view this content.

Mission Critical Video over LTE (FS_MCVideo): This includes enabling broadband features like video group communication (to enable see what I see), video broadcast, and video consolation to allow a PS UE to view a video with video recorder functionalities and manage several video streams in single operation. To accomplish this, the FC_MCVideo aims at reusing existing standards when possible and justified, including the MCPTT framework (*e.g.,* call commencement, call termination, security, and user management). The FC_MCVideo requirements include the use of ProSe, security, confidentiality, interaction with MCPTT voice services for same functions like group management, group communication involving several media types (e.g., a user with voice commenting a video), and fall back mode in case of scarce resources (e.g., possibility of transmitting a sound or commentary associated with a video).

Mission Critical Data over LTE (FS_MCDATA): Some of the requirements for this are inherited from different organizations like The Critical Communications Association (TCCA), APCO, OMA (Push-to-talk over Cellular (PoC) version 2.1 and PCPS), and The European Telecommunications Standards Institute (ETSI) TETRA and Critical Communications Evolution (TCCE) user requirements. Most potential requirements are almost the same as of FC_MCVideo.

1.3.1.8 Release 15: 3GPP release 15 provides further enhanced MCPTT group call procedure and provides a support to integrate legacy PSNs to cellular networks Kaleem et al. (2018).

1.3.2 Open Mobile Alliance

Open Mobile Alliance (OMA) is an industry forum that develops open specifications for enablers of new mobile services. The main objective for these specifications is to enable interoperability across different networks, regions, devices, and managing entities. OMA Communications Working Group (OMA COM WG) has defined multiple broadband Push to Talk (PTT) standards for commercial cellular networks and more recently for PSNs. We now briefly highlight other broadband PTT standards defined by OMA in past Ferrus & Sallent (2015).

1.3.2.1 PTT over Cellular: PTT over Cellular (PoC) is OMA's first broadband PTT standard for commercial cellular networks that has less stringent constraints on performance than PSNs Alliance (2006). This two-way radio standard provides support for immediate one-to-one and one-to-many communication. PoC is based on IMS and thus can be implemented on top of both 2G and 3G mobile systems.

After its first release in 2008 (v1.0), the standard was revised multiple times in 2009 (v1.04) 2011 (v2.0, v2.1) to incorporate new features. These features include support for automatic and manual answering modes, transmission of multimedia other than voice (such as text, files, videos, and images), and interconnection with external PTT networks. Although PoC is a commercial cellular standard, its latest version (v2.1) took initial steps towards providing mission-critical features desired for PS community such as the ability to communicate in ad-hoc mode, a multicast group or a pre-defined group. Furthermore, it can prioritize communications, allows preemption, and supports dispatcher functions.

1.3.2.2 Push to Communicate for Public Safety (PCPS): PCPS is a newer standard from OMA to support both PS and commercial communications. It consolidates all features from PoC and extends them to work with LTE advanced (i.e., 3GPP Release 12). In 2015, OMA licensed PCPS V1.0 specifications to 3GPP for using it in defining Mission Critical Push to Talk (MCPTT) functionality within LTE standard.

With its close ties to other SDOs like 3GPP, OMA actively participated in defining MCPTT, a broadband PTT standard finalized in Release 13 of 3GPP that is discussed later in this section.

1.3.3 Alliance for Telecommunication Industry Solutions

Alliance for Telecommunication Industry Solutions (ATIS) is one of the organizational partners of 3GPP that develops standards and solutions for Information and Communication Technology (ICT) industry. ATIS is working to support the transition of PS applications from legacy circuit-switch networks to all-IP networks Zentner et al. (2015). It realizes that several industrial sectors such as energy and utility, building alarms systems, public transportation, and emergency management services connect to PS agencies using legacy and non-standardized communication networks. These systems are capable of transporting voice, collecting sensed values, and applying supervisory control. However, their proprietary and application-specific nature makes them expensive and their horizontal integration a real challenge. The transition to All-IP is considered to protect critical infrastructure more reliably, assure interoperability across multiple applications, and reduce response time for handling emergencies in natural or man-made disasters.

In what follows, we highlight the targeted sectors of ATIS for all-IP transitions.

1.3.3.1 Energy and Utility Sector: In this PS sector, two communication solutions were proposed to replace PSTN copper wires. The first solution is based on an IP private line that can provide carrier-grade performance. The second is a wireless solution that deploys private wireless network across the entire grid. It is designed for network monitoring and system backup.

1.3.3.2 Building Alarm Systems: Police, fire brigade, and private security services usually respond to alarms triggered by private and public buildings and protected places such as airports and military installation to prevent loss of human life or property. Many of these alarms are still connected to the first responders using legacy circuit switched system. The first solution to migrate to IP is provided by a module that can transmit alarms to first responders and can continuously monitor IP connections with the server as well. The second is a Machine-to-Machine based solution geared with a secure cellular (3G/4G) connectivity capable of reporting alarms, device status, and diagnostic information.

1.3.3.3 PS Communication with Emergency Centers: The evolution of PS wireless communication is already underway, as highlighted by standardization activities of 3GPP and OMA. In parallel to this, the integration of PS communication (e.g., fire, p, and EMS etc.) with Emergency Management Centers needs serious attention. ATIS has some roles in proposing the following solutions as a milestone towards migration to next-generation emergency services.

- Multiple broadband solutions for communication between state and federal emergency management agencies.
- An IP-based system that integrates with an emergency center and radio dispatch via IP network.
- Multiple solutions for Next Generation (NG) 911, supporting migration of analog to IP-based communications.
- Secure solution for call delivery using softswitch routing, enhanced call handling, and secure IP networks.
- Voice over IP (VoIP) based solution for communication with existing E911.

1.3.3.4 Smart City Solutions: PS is not the basis for smart city design and initial implementation, but there are opportunities for leveraging these deployments to support PS. In addition to working on mentioned PS sectors, ATIS, in collaboration with 3GPP, has initiated two standardization programs that will contribute to the long-term roadmap for PS applications: 5G-evolution and cybersecurity. These programs include solutions from different technology innovations like IoT, cloud applications, and Software-Defined Networking (SDN). The 5G-evolution program includes enhancements to redundancy and resiliency, security across networks, and capacity management during planned events and emergency response situations. Cybersecurity is accessing cutting-edge technologies that can contribute innovative cybersecurity solutions in the future. These technologies include network virtualization, SDN, cloud architectures, and enhanced end-user control.

1.3.4 APCO Global Alliance

Association of Public-Safety Communications Officials (APCO) is an international organization of PS communication professionals that establishes standards, solutions, and guidelines for interoperable, narrowband LMR/PMR systems in the areas of cybersecurity, Next Generation 911 (NG991), and the telematics Baldini et al. (2014).

As part of their standardization efforts, APCO developed guidelines for the prevention of various cyber attacks on the IP-based PSNs and communications. This includes the prevention of Denial-of-Service (DoS) attack, swatting/spoofing, and network intrusion attack. Swatting/Spoofing is the spoofing of the caller's ID to trick the emergency services to dispatch personnel to a fake incident.

Another contribution from APCO is the development of standards and guidelines in the area of vehicle telematics, which includes the handling of Advanced Automatic Crash Notification (AACN) calls from Telematics Service Providers (TSPs). The standard allows each agency to define their own policies for AACN call handling and dispatch.

APCO has also dedicated its efforts to develop standards for new forms of communication to 911 such as text-to-911 and mobile apps. The text-to-911 is an interim solution, which processes text messages to 911 via carrier native SMS. The solution does not depend on vendor-specific applications implemented in individual PSAPs (PS Answering Points). The solution provides direct access to 911 PSAPs for individuals having speech disabilities. Moreover, APCO is working to develop guidelines for the development of mobile applications, which can securely communicate with 911 centers. These mobile apps will use the public Internet, which can be a security threat to the NG911 network. The standard should ensure the security and reliability of NG911 centers.

In short, 911 is gradually transiting to IP-based networks, which will enable the use of text, videos, and mobile apps with better security and reliability and APCO is playing its part to effectively integrate these new forms of communications to next-generation 911.

1.3.5 Groupe Speciale Mobile Association (GSMA)

GSMA, an association of mobile operators, supports the standardization of GSM system. Its Voice over LTE (VoLTE) solution was fully standardized in 2000 Tanaka & Koshimizu (2012) to provide a single digital packet service capable of transferring both data as well as voice over LTE networks using IP. VoLTE is built on top of the IP Multimedia Subsystem (IMS) Tanaka & Koshimizu (2012), a standard from 3GPP for providing multimedia services over cellular networks.

VoLTE provides a single homogeneous service for transferring both data and voice using IP, which eliminates the dependence on 2G/3G including the circuit-switched network. As a result, VoLTE provides features such as better spectrum utilization, higher voice quality, and better security. All these features make it an attractive option for PS networks as noted in Tanaka & Koshimizu (2012) and industry is pushing it to become part of future PS networks. In addition, VoLTE provides wireline-quality voice services to LTE users, which is essential for mission-critical applications in PSNs. Nevertheless, its current specifications do not incorporate important PS features such as group communication, push-to-talk, and delivery of video among group Câmara & Nikaein (2015), an important gap that is bridged by the features introduced by 3GPP in releases 12-13 as discussed earlier.

Apart from standardization efforts from different SDOs, there is a need to develop a partnership across the industry to facilitate a transition pathway for critical applications. Although the manufacturers, network operators, emergency management agencies, and SDOs are providing different solutions, it is equally important to take a longer-term view of how this network evolution will present new opportunities and benefits that could be realized by the PS sector. It is important to note that in the PS sector, important attributes such as reliability, resilience, latency, diversity, etc. will not be bounded by the performance characteristics of a single network (e.g., access or core), rather the IP-enabled networks and devices will provide additional capabilities and media alternatives that, if designed properly, can provide a next-generation of PS applications.

1.4 Future Challenges and Enabling Technologies

The future PSN will be an inclusive system that will include different technologies, such as legacy professional mobile radio (Private Mobile Radio (PMR) in the UK and LMR in North America), massive IoT, commercial cellular networks, WSNs, Machine-to-Machine (M2M) communications, D2D communications, ad-hoc networks, satellite networks, aerial eNodeBs, OSNs, big data, and many others. The legacy PSNs will coexist with LTE for quite a long time until the new network is 100% flaw proof. This complete system will be a part of 5G networks, where SDN will play a vital role in managing and operating this heterogeneous network in terms of technology both in access and core. All-IP based solutions in the access and NG 911 in core network will help to make this complex informative system interoperable and integrated.

Massive IoT will be a part of the network, which will help to report critical incidents to NG911 without any human involvement. Location-based services will help to locate the site and the magnitude of the incident. D2D communications will keep the necessary communication until drones equipped with aerial eNodeB reach the site. The first responders will be able to communicate with each other and central station using D2D communication, aerial eNodeBs, and Satellite communications.

Social media will be another tool to report incidents to NG911. Cloud computing and big data analytics tools will play a critical role in PS agencies' ability to detect and respond to threats.

The complete ecosystem of PSN will enable real-time access to the information, where content-rich database lookups and remote analytics will lead to greater productivity and reduced costs. The system will enable broadband access to the PS officials to keep them connected anywhere and anytime. Mission critical data over LTE will give first responders capabilities to transmit a massive amount of data to and from command centers and/or directly among each other.

The ecosystem will greatly increase the utility and offer access to a whole array of advanced multimedia applications like bi-directional vehicular video, locationaware real-time services, mobile office, in-field productivity, multimedia command and control, dynamic mapping, weather and traffic flows, Content-rich lookups to complex databases, and many others.

1.4.1 Future Challenges

PPDR organizations include law enforcement agencies, emergency management agencies, fire departments, Emergency Medical Services (EMS), rescue squads, and many others. These organizations make the use of the ICT sector for their day-to-day communications and rescue operations. The ICT sector for PS communication includes legacy PSNs (*i.e.,* PMR/LMR) systems, broadband PSNs systems, massive IoT, commercial cellular networks, WSNs, OSNs, big data, and many others. Incorporating these diverse ICT technologies into PSNs poses different challenges. In the following section, we discuss the possible challenges and enabling technologies for future public safety networks.

1.4.1.1 Connectivity: PSNs must ensure uninterrupted connectivity in case of disasters. In disaster situations, the ICT infrastructure may be damaged with fewer nodes available to support high volumes of traffic causing overloading. Therefore, it is essential to define the specific roles of each integrated technology, such as PS agencies (police, fire brigade, ambulance, *etc.*), legacy PSNs (PMR/LMR), commercial cellular networks and other, before, during, and after disasters. The techniques of Self-Organizing Networks (SONs) can be employed to provide uninterrupted service to first responders during disasters.

D2D communications can be the first option with aerial eNodeBs are deployed in the affected area Moghaddam et al. (2018). An efficient solution for vertical handoff between D2D communications, aerial eNodeB, Satellite Communication, and Wireless LAN must be designed to ensure uninterrupted connectivity. Instead of completely relying on these infrastructure-centric solutions for public safety, we can consider opportunistic networks Lu et al. (2016), Pelusi et al. (2006) in disaster situations. Haggle Scott et al. (2006) is a typical example, which is an asynchronous data-centric network architecture based on the publish-and-subscribe model.

1.4.1.2 Interoperability: Interoperability is the ability of first responders from different PPDRs to communicate and share information in real time. The interoperability is mainly due to proprietary solutions from local PPDRs and lack of standards for public safety communications. The use of commercial cellular networks in public safety is emerging as one possible solution to solve interoperability problems. However, sharing communication infrastructure is not enough to completely solve the interoperability problems. All IP-based solutions and common backhaul like NG 911 are needed to interoperate different PPDRs and communication technologies to share networks, data, and resources in an efficient way.

1.4.1.3 Resource Scarceness: Due to the increased number of PS organizations with their own network infrastructure, PSNs may undergo resource scarceness. In addition, voice traffic registered over commercial cellular networks in the areas affected by disasters increases during and after disaster Gebremariam et al. (2018). Future public safety networks sharing resources with commercial cellular networks can go resource scarce in the times of disaster. Simply allocating more radio resources to public safety networks does not solve the issue of spectrum efficiency. New techniques for dynamically allocating radio resources like SDN must be adopted. Moreover, techniques like cognitive radio can further help to improve the spectrum efficiency of public safety communications.

1.4.1.4 Security: Public safety networks must be secured from malicious attacks Portmann & Pirzada (2008). The existence of interconnectivity and interoperability of different agencies, communication technologies, coworkers, video surveillance, D2D networks, and WSNs results in a complex automated information system and introduces new security risks in public safety networks. The end-to-end security of inter-agency and cross-border communication will be a great challenge in future public safety networks.

Network sharing with commercial cellular networks will further tighten security requirements in public safety networks. In shared networks, public safety services must have their own mechanism for user authentication and authorization, which should be managed by public safety service providers. For better security, the traffic from different public safety agencies must also be separated from each other. A better solution for interoperability will facilitate the implementation and enforcement of end-to-end security. Several layers of protection must be provided to secure public safety networks including application such as physical layer security Hamamreh et al. (2018), data encryption Asghar et al. (2014), and management-interface security.

1.4.1.5 Big Data: Traditionally, the data used by public safety officials was static in nature such as the police department's record and the court information system etc. However, this is not the case with OSNs today where there is a need to monitor issue-based social media traffic across the universe of social media users. Another challenge in personnel security screening, where names are searched against law enforcement databases as well as against social media, and open source information. This pushes the responsibilities of public safety officials into the territory of "big data", where the volume, variety, and velocity of data outstrip the ability of the unaided analyst to deal with it.

On the other hand, the emergency centers like 911 do not support technology beyond caller ID and location-based information. So the next generation 911 centers must be able to receive and analyze a wide array of media-rich contents because many individuals simply report the incident on social media without contacting 911 directly, assuming that someone else has already done so.

1.4.2 Enabling Technologies

The interoperability of different agencies, communication technologies, legacy and broadband PMR networks, video surveillance, D2D networks, and wireless sensor networks results in a complex automated information system that needs to be managed in an efficient way in order to accomplish the aforementioned challenges. Following technologies can offer guaranteed and optimized spectrum, end-to-end security, uninterrupted connectivity, and resilience.

1.4.2.1 Software-Defined Networking: SDN will be one of the key enablers for this multi-technology and multi-agency complex informative system of future public safety networks. A central controller possibly residing in NG911 centers will help to make the intelligent decisions for technology selection in time of disaster. This will also help to separate traffic from different agencies with controlled interconnection interfaces between agencies. It will further increase the spectrum efficiency of the system by dynamically allocating radio resources among different technologies (like D2D and cellular) and agencies.

1.4.2.2 Cognitive Radio Networks: Cognitive Radio Networks (CRNs) will help to efficiently utilize radio resources among Primary Users (PUs) and Secondary Users (SUs). In an underlay CRN setting, the SUs will be allowed to share the spectrum with the PUs under the condition that the interference observed at the PU is below a predetermined threshold. A practical example for such networks would be an indoor femto-cell where the users will be allowed to deploy femto Base Stations (BSs) that will have the ability to share the spectrum with macrocell users. Such networks will prove to have an optimized spectrum utilization with uninterrupted connectivity Ansari et al. (2014). Moreover, cooperative beamforming in Multiple-Input and Multiple-Output (MIMO) CRNs will help to incorporate physical layer security in the nodes and protect information from possible eavesdropping and/or jamming, especially in D2D case.

1.5 Conclusion

The chapter provided a very broad coverage of standardization efforts on PSNs. It spans well beyond the recent standards ratified by 3GPP as part of defining the 5^{th} generation of cellular communications. This choice reflects the fact that other SDOs and their earlier standards have played a vital role in shaping the recent standardization of communication for PSNs in 5G. Many challenges still remain to be overcome. Some challenges arise from lack of a single well-adopted standard that necessitates a co-existence of multiple standards in the foreseeable future and the requirement of connecting them in a way to offer the best performance as well as efficient utilization of scarce radio spectrum. The future revisions of the 5G standards would continue to look into these aspects.

Bibliography

Ahmadi, S. (2013), *LTE-Advanced: a practical systems approach to understanding 3GPP LTE releases 10 and 11 radio access technologies*, Academic Press.

Alliance, O. M. (2006), ‘Push to talk over Cellular (PoC)-Architecture’, *OMA-AD-PoC-V1 0-20060609-A* .

Ansari, I. S., Abdallah, M. M., Alouini, M.-S. & Qaraqe, K. A. (2014), A performance study of two hop transmission in mixed underlay RF and FSO fading channels, *in* ‘Proceedings of the 2014 IEEE Wireless Communications and Networking Conference (WCNC’ 2014)’, IEEE.

Asghar, M. R., Gehani, A., Crispo, B. & Russello, G. (2014), PIDGIN: Privacy-preserving interest and content sharing in opportunistic networks, *in* ‘Proceedings of the 9th ACM symposium on Information, computer and communications security’, ACM, pp. 135–146.

Baldini, G., Karanasios, S., Allen, D. & Vergari, F. (2014), ‘Survey of wireless communication technologies for public safety’, *IEEE Communications Surveys & Tutorials* **16**(2), 619–641.

Buis, M. (2012), ‘LTE-Advanced Release-10 Features Overview’, *adare GmbH* .

Câmara, D. & Nikaein, N. (2015), *Wireless Public Safety Networks Volume 1: Overview and Challenges*, Elsevier.

Farrill, F. C. (2012), 'FirstNet Nationwide Network (FNN) proposal', *First Responders Network Authority, Presentation to the Board* .

Ferrus, R. & Sallent, O. (2014), 'Extending the LTE\/LTE-A business case: Mission- and business-critical mobile broadband communications', *IEEE Vehicular Technology Magazine* **9**(3), 47–55.

Ferrus, R. & Sallent, O. (2015), *Mobile broadband communications for public safety: The road ahead through LTE technology*, John Wiley & Sons.

Gebremariam, A. A., Usman, M., Bassoli, R. & Granelli, F. (2018), 'SoftPSN: Software-defined resource slicing for low-latency reliable public safety networks', *Wireless Communications and Mobile Computing* **2018**.

Hamamreh, J. M., Furqan, H. M. & Arslan, H. (2018), 'Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey', *IEEE Communications Surveys Tutorials* pp. 1–1.

Hoymann, C., Astely, D., Stattin, M., Wikstrom, G., Cheng, J.-F., Hoglund, A., Frenne, M., Blasco, R., Huschke, J. & Gunnarsson, F. (2016), 'LTE release 14 outlook', *IEEE Communications Magazine* **54**(6), 44–49.

Kaleem, Z., Yousaf, M., Qamar, A., Ahmad, A., Duong, T. Q., Choi, W. & Jamalipour, A. (2018), 'Public-safety LTE: Communication services, standardization status, and disaster-resilient architecture', *arXiv preprint arXiv:1809.09617* .

Lu, Z., Cao, G. & La Porta, T. (2016), Networking smartphones for disaster recovery, *in* 'Pervasive Computing and Communications (PerCom), 2016 IEEE International Conference on', IEEE, pp. 1–9.

Moghaddam, J. Z., Usman, M. & Granelli, F. (2018), 'A device-to-device communication based disaster response network', *IEEE Transactions on Cognitive Communications and Networking* .

Parkvall, S., Furuskar, A. & Dahlman, E. (2011), 'Evolution of LTE toward IMT-advanced', *IEEE Communications Magazine* **49**(2).

Pelusi, L., Passarella, A. & Conti, M. (2006), 'Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks', *IEEE communications Magazine* **44**(11).

Portmann, M. & Pirzada, A. A. (2008), 'Wireless mesh networks for public safety and crisis management applications', *IEEE Internet Computing* **12**(1).

Roessler, J. (2015), 'Lte-advanced (3gpp rel. 12) technology introduction white paper', *München: Application Note-1MA252-Rohde & Schwarz International* .

Sauter, M. (2017), *From GSM to LTE-advanced Pro and 5G: An introduction to mobile networks and mobile broadband*, John Wiley & Sons.

Scott, J., Crowcroft, J., Hui, P. & Diot, C. (2006), Haggle: A networking architecture designed around mobile users, *in* 'WONS 2006: Third Annual Conference on Wireless On-demand Network Systems and Services', pp. 78–86.

Tanaka, I. & Koshimizu, T. (2012), 'Overview of GSMA VoLTE Profile', *NTT Docomo Technical Journal* **13**(4), 45–51.

Usman, M., Gebremariam, A. A., Granelli, F. & Kliazovich, D. (2015), Software-defined architecture for mobile cloud in device-to-device communication, *in* 'Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2015 IEEE 20th International Workshop on', IEEE, pp. 75–79.

Usman, M., Gebremariam, A. A., Raza, U. & Granelli, F. (2015), 'A software-defined device-to-device communication architecture for public safety applications in 5G networks', *IEEE Access* **3**, 1649–1654.

Zentner, M. H., Frommelt, B. J., Horwath, G. J., Mafera, P. F. & Sawicki, D. J. (2015), 'Method to provide context-aware linkage between NG9-1-1 SMS and public safety incident'. US Patent 9,148,771.